FORTINET
High Performance Network Security

FortiToken Mobile for Android

Release Notes

VERSION 4.0

FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

3/31/2017

FortiToken - Release Notes for Android FortiToken Mobile 4.0

33-400-412648-20170331

TABLE OF CONTENTS

Introduction **4**
What's New **5**
Push notifications 5
Fingerprint scanner login 5
Permissions 5
Product support **8**
Android version support 8
FortiOS and FortiAuthenticator support 8
FortiToken platform scalability 8
Registering FortiToken Mobile **10**
Known issues **11**

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions and caveats, resolved and known issues for FortiToken Mobile for Android, version 4.0, build 0032.

FortiToken Mobile is an OATH compliant, time-based one-time password (OTP) generator application for mobile devices. FortiToken Mobile produces its one-time password (OTP) codes in an application that you can download to your Android, iOS, or Windows mobile device without the need for a physical token.

Go to the Google Play store to download the free FortiToken Mobile application for Android.

For additional documentation, please visit: http://docs.fortinet.com/fortitoken/

What's New

Before upgrading, review the following changes for impact to your unique deployment. Note that this list is not exhaustive but highlights the major feature enhancements in this release.

Push notifications

Push notifications for approving or denying login attempts is now supported. Push technology allows you to receive login attempt notifications on your smartphone or tablet and verify the login with a single tap.

Push notifications are used to send alerts to the end-user's device each time a login request is made. The alert contains information about the login attempt, for example the location from which the attempt originated. The user simply taps to approve or deny the request. If approved, a new OTP is automatically generated and sent by FTM to transparently authenticate the end-user in the background. If denied, FTM automatically sends an alert to the System Administrator.

The manual OTP authentication method is still available in case the end-user cannot or does not wish to use PUSH.

When upgrading, users will see a request to allow notifications. This is required for PUSH notifications to work.

Fingerprint scanner login

Fingerprint scanning is now supported for local authentication into the FTM application.

Permissions

The following section shows information on the permissions requested for FTM for Android and what functions they are used for.

Static permissions requested for this build:

Function	Permission
QR Barcode scanning and TouchID	<uses-permission android:name="android.permission.CAMERA"/> <uses-permission android:name="android.permission.USE_ FINGERPRINT"/>

Function	Permission
Accessing the Internet including communication to register FortiTokens with FortiCare	<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/> <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/> <uses-permission android:name="android.permission.INTERNET"/>
"Send Feedback by Email", to automatically populate the "Sender" field, and if Gmail is the default/used email client	<uses-permission android:name="com.android.email.permission.ACCESS_PROVIDER"/> <uses-permission android:name="com.android.email.permission.READ_ATTACHMENT"/> <uses-permission android:name="com.google.android.gm.email.permission.ACCESS_PROVIDER"/> <uses-permission android:name="com.google.android.gm.email.permission.READ_ATTACHMENT"/> <uses-permission android:name="com.google.android.gm.email.permission.READ_ATTACHMENT_PREVIEW"/> <uses-permission android:name="com.google.android.gm.permission.READ_CONTENT_PROVIDER"/> <uses-permission android:name="com.google.android.gm.permission.READ_GMAIL"/> <uses-permission android:name="com.google.android.gm.permission.WRITE_GMAIL"/> <uses-permission android:name="com.google.android.providers.gmail.permission.READ_ATTACHMENT"/> <uses-permission android:name="com.google.android.providers.gmail.permission.READ_GMAIL"/>

Function	Permission
Internally share files between applications *	<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/> <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/> <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
Internal use **	<uses-permission android:name="android.permission.WAKE_LOCK"/> <uses-permission android:name="android.permission.VIBRATE"/> <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
Receive Push notifications from Google Services	<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/> <uses-permission android:name="com.fortinet.android.ftm.permission.C2D_MESSAGE"/>

* For example, FortiToken prepares an attachment to be sent by email for "Send Feedback by Email". Depending on the implementation, the QR barcode or TouchID might need to share images too.

** For example, FortiToken must keep the phone awake while it is upgrading the internal database to avoid data corruption.

Product support

Android version support

The following Android versions are supported:

- 4.4.x
- 5.x
- 6.x
- 7.x

FortiOS and FortiAuthenticator support

FTM requires FortiOS 5.0 and up and/or FortiAuthenticator 1.4 and up.

FortiToken platform scalability

The following table shows the maximum number of FortiTokens that can be assigned to certain FortiGate and FortiAuthenticator models. Note that FortiToken is also supported on specific FortiWiFi models.

All data for this table was taken from the following Product Matrix datasheet.

FortiGate Models	Max. FortiTokens
30E	20
50E / 60D / 60E / 70D / 80D / 90D / 90E	100
100D / 100E / 200D / 200E / 300D / 500D / 600D / 800C / 900D	1,000
1000D / 1200D / 1500D / 2000E / 2500E / 3000D / 3100D / 3200D / 3700D / 3800D / 7040E VMware / Xen / AWS / AWS on Demand / KVN / Hyper V	5,000

FortiAuthenticator Models	Max. FortiTokens
200E	500
400E	2,000
1000D	10,000

FortiAuthenticator Models	Max. FortiTokens
2000E	20,000
3000D / 3000E	40,000
VM BASE to VM-100000-UG	200 to 200,000+

Registering FortiToken Mobile

You will need a certificate to register FortiToken Mobile. There are two options for getting FortiToken Mobile certificates for use on your authentication server: FortiToken Mobile Redemption Certificate, and FortiToken Mobile Free Trial “virtual” certificate.

For each FortiToken Mobile purchase, you will receive a physical redemption certificate. Scratch off the designated area of the redemption certificate to reveal the 20-digit activation code.

The following steps show how to register FortiToken Mobile on a FortiGate and FortiAuthenticator.

On the FortiGate

1. Locate the 20-digit code on the redemption certificate.
2. Go to **User & Device > FortiTokens** and select **Create New**.
3. Select **Mobile Token**, and enter the 20-digit certificate code in the **Activation Code** box.
4. Select **OK**.

On the FortiAuthenticator

1. Locate the 20-digit code on the redemption certificate.
2. Go to **Authenticaton > User Management > FortiTokens** and select **Create New**.
3. Select **FortiToken Mobile**, and enter the 20-digit certificate code in the **Activation codes** box.
4. Select **OK**.

To ensure messaging functions properly, you must configure the messaging server, configure users to receive messages from the server by email or SMS, and provision FortiToken Mobile for the user on the FortiGate and/or FortiAuthenticator.

To see more information on how to provision FortiToken Mobile for a user on a FortiGate and FortiAuthenticator, see the FortiToken Comprehensive Guide.

For more information see the FortiToken Mobile product datasheet available on the Fortinet web site at https://www.fortinet.com/products/identify-and-access-management/network-authentication/fortitoken-mobile.html

Known issues

This section lists the known issues of this release, but is not a complete list.

For inquires about a particular bug, please contact Fortinet Customer Service & Support: https://support.fortinet.com

Bug ID	Description
286347	App does not time out and prevents device from sleeping.
405353	[FortiToken Android] Device PIN should be an alternative for touchID if it is not available.
405839	[FortiToken Android] front camera on Nexus7 cannot activate token by scanning QR image.
406246	Should directly show token list view if pass the device pin authentication.
406436	App opens when receive push notification from background.
407439	Should change the error message for "don't allow take pictures" permission.
407739	Should throw message "PIN doesn't match and try again" if user enters the wrong PIN.
407760	[FTM Android] App does not display any user friendly message for failing PINs.
408986	TouchID UI issue in split screen.
408988	[FortiToken Android] crash issue in split screen.
410772	Should not show "Enable TouchID" popups if checks "do not show this message again".
410800	Should need three permissions for FTM android app. For more details, see Permissions in the What's New section.
411246	"enter the current PIN" view should not show/flash if press [cancel] on touchID view.
411270	FTM android app bypasses the PIN if the pin length is not default 4-digits in FACb.
411492	Incorrect view shows up when send push from background .
411610	FAC should not determine PIN length if no PIN is required.

Bug ID	Description
411672	The "touchID auth" view is not be able to show when send push and device is locked. **Workaround:** Unlock the device without double tapping on the Push notification. If the user taps on the push banner and then unlocks device, the user cannot see the push in the top-right comer. If the user doesn't tap on the push banner (i.e just directly unlocks the device), the user is able to approve the login attempt.
411892	FortiToken Android]:"idle for 60 seconds" show up in the incorrect time.